## Contents

**Introduction to CREST Crypto-Math Project** .......................... 1  
Tsuyoshi Takagi

**Part I  Mathematical Cryptography**

**Multivariate Public Key Cryptosystems** .......................... 17  
Yasufumi Hashimoto

**Code-Based Zero-Knowledge Protocols and Their Applications**  .... 43  
Kirill Morozov

**Hash Functions Based on Ramanujan Graphs**  ................. 63  
Hyungrok Jo

**Pairings on Hyperelliptic Curves with Considering Recent Progress on the NFS Algorithms**  .. 81  
Masahiro Ishii

**Efficient Algorithms for Isogeny Sequences and Their Cryptographic Applications**  .. 97  
Katsuyuki Takashima

**Part II  Mathematics Towards Cryptography**

**Spectral Degeneracies in the Asymmetric Quantum Rabi Model**  .. 117  
Cid Reyes-Bustos and Masato Wakayama

**Spectra of Group-Subgroup Pair Graphs**  ......................... 139  
Kazufumi Kimoto

**Ramanujan Cayley Graphs of the Generalized Quaternion Groups and the Hardy–Littlewood Conjecture**  .. 159  
Yoshinori Yamasaki
Uniform Random Number Generation and Secret Key Agreement for General Sources by Using Sparse Matrices .............. 177
Jun Muramatsu and Shigeki Miyake

Mathematical Approach for Recovering Secret Key from Its Noisy Version ............................................. 199
Noboru Kunihiro

Part III Lattices and Cryptography

Simple Analysis of Key Recovery Attack Against LWE ............... 221
Masaya Yasuda

A Mixed Integer Quadratic Formulation for the Shortest Vector Problem .................................................... 239
Keiji Kimura and Hayato Waki

On Analysis of Recovering Short Generator Problems via Upper and Lower Bounds of Dirichlet $L$-Functions: Part 1 ............. 257
Shingo Sugiyama

On Analysis of Recovering Short Generator Problems via Upper and Lower Bounds of Dirichlet $L$-functions: Part 2 .......... 279
Shinya Okumura

Recent Progress on Coppersmith’s Lattice-Based Method: A Survey ............................................................. 297
Yao Lu, Liqiang Peng and Noboru Kunihiro

Part IV Cryptographic Protocols

How to Strengthen the Security of Signature Schemes in the Leakage Models: A Survey ............................... 315
Yuyu Wang and Keisuke Tanaka

Constructions for the IND-CCA1 Secure Fully Homomorphic Encryption ...................................................... 331
Satoshi Yasuda, Fuyuki Kitagawa and Keisuke Tanaka

A Survey on Identity-Based Encryption from Lattices .......................... 349
Goichiro Hanaoka and Shota Yamada

Index ................................................................. 367
Mathematical Modelling for Next-Generation Cryptography
CREST Crypto-Math Project
2018, VIII, 368 p. 23 illus., 6 illus. in color., Hardcover
ISBN: 978-981-10-5064-0